FORTINET®

High Performance Network Security

A Look at Layered Security

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Wednesday, March 25, 2015

A Look at Layered Security

Table of Contents

Introduction

Your FortiGate has just arrived. You've taken it out of its box and connected it to your network. All you need to do now is configure it to protect your network, which raises some questions: what features should you use, how should you use them, and most importantly, *why*?

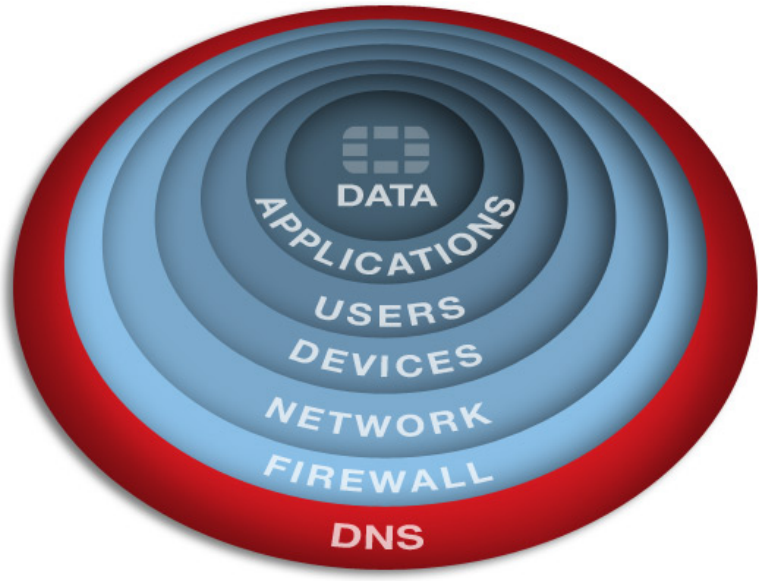
In this document, you'll find the answers to the following questions, as you learn about layered security and how to apply it using your FortiGate:

This document was original published as a series of articles on the Fortinet Blog.

What is Layered Security?

Layered security combines multiple security measures together to make sure that you don't have all your security eggs in one basket. This keeps you safe from both different sources and different types of threats.

There are a few different models out there for layered security. The one we'll be using has seven distinct layers that offer different methods of protection. Below you'll find a brief description of each layer, followed by a list of the relevant Fortinet features.



Layer 1: DNS

A Domain Name System (DNS) acts like a phone book to help your computer find websites. A DNS server is typically provided by your ISP, but for more security, you can use a secure DNS server. By default, the FortiGate uses FortiGuard as a secure DNS server, so this layer is already covered for you right out of the box.

FortiGate Features: FortiGuard DNS server

See "How do I secure the DNS Layer?" on page 7

Layer 2: Firewall

A firewall acts as a filter between your network and the outside world by scanning all network traffic and deciding what traffic to let in or out. You can configure FortiGate firewall policies (also called 'security policies') to control your user's Internet access.

FortiGate Features: Firewall policies

See "How do I create a Firewall Policy?" on page 11.

Layer 3: Network

The network layer focuses on monitoring the signs of various external threats that can often evade your firewall's defenses. There are many known types of these attacks and new ones appear every day. Your FortiGate can protect you against these attacks by using FortiGuard's regularly updated database to recognize and, if necessary, block the traffic that contains the threat.

FortiGate Features: Intrusion Prevention System (IPS), denial of service (DoS) policies

See "How Do I Protect Against External Attacks?" on page 16.

Layer 4: Devices

Having a firewall for your network doesn't guarantee protection for the individual devices on your network. Applying firewalls to your devices ensures that the devices are always protected, even in the event that the firewall fails.

To make sure all your network devices are protected, the FortiGate uses Endpoint Control to block unprotected devices from accessing the network. Device types can also be identified so that you can limit the access of less secure devices, such as mobile phones.

FortiGate Features: Endpoint control, device authentication, vulnerability scanner

See "How Do I Keep Network Devices Secure?" on page 19.

Layer 5: Users

Most people think that network security is primarily done to counter outside threats. However, the percentage of threats from external sources is only around 10-20%. You are far more likely to be compromised internally, either through human error, carelessness, or ill intent.

The user layer is often the trickiest to manage, due to the need for a balance between security and convenience. As such, the best defense against internal threats is awareness and education.

Unfortunately, this alone may not be enough, which is why your FortiGate has a number of security features to keep your network secure from internal threats. You can also use a variety of authentication methods to identify network users and allow varying levels of access, depending on the user’s needs.

FortiGate Features: AntiVirus, web filtering, user authentication, Fortinet single sign-on (FSSO)

Layer 6: Applications

It is very important that your software applications come from trusted and reliable sources and that all of your applications, as well as operating systems, are kept up-to-date in order to protect your network from newly discovered exploits.

You can also use your FortiGate's application control to prevent certain application types that could put your network at risk, such as peer-to-peer downloading applications, from running.

FortiGate Features: Application control

Layer 7: Data

In the Information Age, the computer is much less valuable than the data it stores. Data Leak Prevention (DLP) allows your FortiGate to ensure that vital information is not allowed beyond the network.

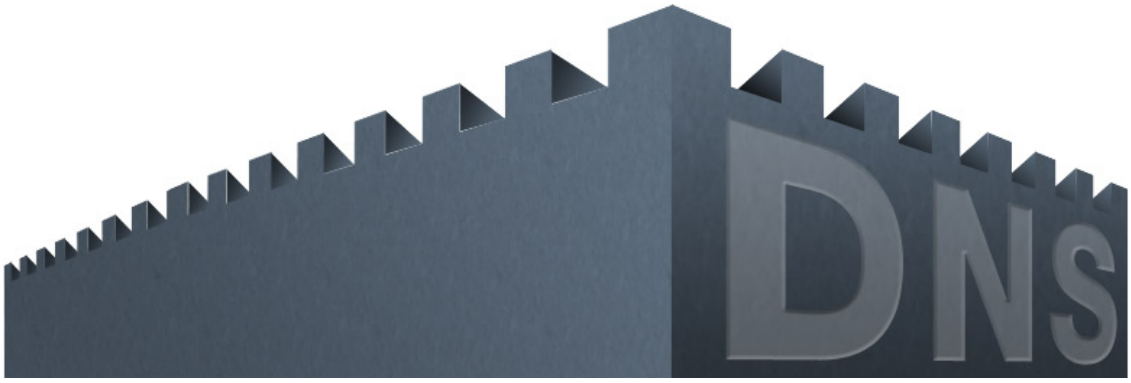
To increase security, data should be encrypted and password-protected, such that if someone does manage to access your data, they aren't able to do anything with it.

In addition, always back up your data in order to prevent serious data loss.

FortiGate Features: Data Leak Prevention

.

How do I secure the DNS Layer?



Domain Name System (DNS) is used like a phonebook to help your computer find websites by translating a domain name to a website's IP address. For example, the domain name www.fortinet.com is translated to the IP address 66.171.121.34, which lets your computer successfully find the Fortinet site.

The primary roles of a DNS server are to keep a record of domain names and IP addresses, so they can redirect incoming traffic to where it wants to go.

DNS Threats

There are three types of attacks that involve DNS servers:

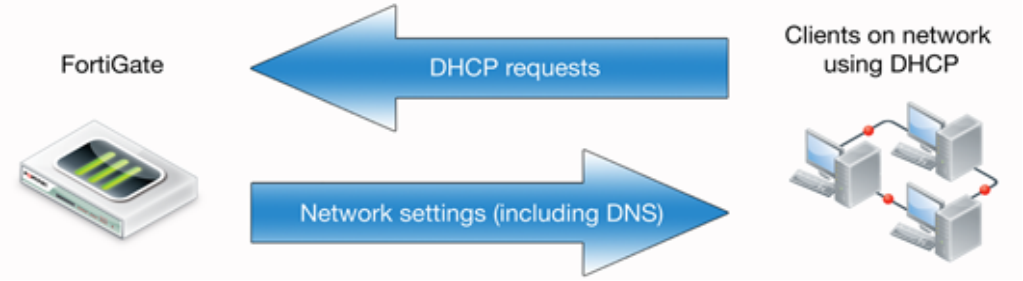
- **Hijacking** occurs when malware changes your network's DNS settings to point to a rogue DNS server that is under the control of the attacker.
- **Cache poisoning** (also called cache pollution) involves a DNS server's records being changed to link a legitimate domain name to a malicious IP address.
- **Spoofing** involves a DNS request being intercepted by an attacker whose response appears to have come from the proper DNS server.

In all of the above attacks, you could be sent to a clone of a legitimate website - perhaps your online banking site - and have your credentials stolen when you try to log in as usual, or have malware downloaded on your computer without your knowledge.

Choosing your DNS Server

The first decision you need to make when choosing a DNS server is whether you should use an external server (and depend on someone else to protect your DNS layer) or manage your own server.

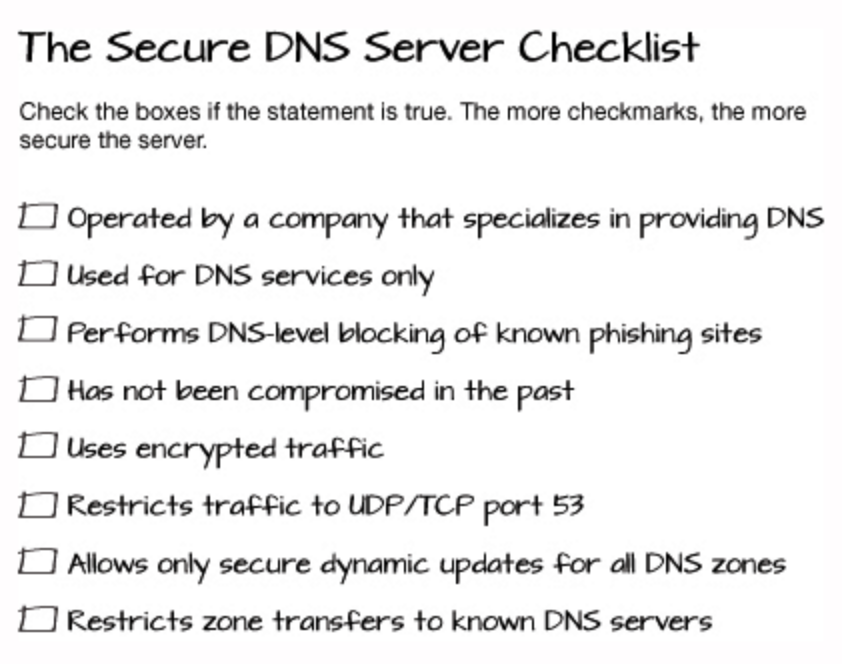
Using an External Server



If your network uses your FortiGate's DHCP server to get IP addresses, then your FortiGate's DNS settings are also used for the entire network. This allows changes to the settings to be made quickly and easily, and means that if your FortiGate is using a secure DNS, your entire network will be too.

By default, your FortiGate uses the FortiGuard DNS servers. This set up is sufficient for many situations; however, there are reasons to use other servers, such as security requirements or performance issues (there are several free diagnostic tools available that allow you to compare DNS server response times).

If you've decided to change from the default to a specific DNS server, here is a quick checklist to help you find one that is secure (and remember, you're going to need two of them in order to have a primary server and a backup server):

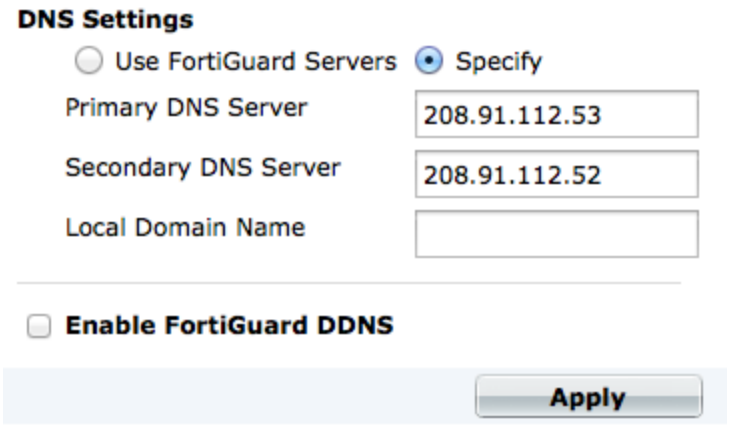


How to Change Your Serve

Once you've chosen two secure servers to use, changing the servers on your FortiGate is simple. All you need is administrative access and the IP addresses of your servers.

To change your DNS servers, do the following:

1. Log into your FortiGate.
2. Go to **System > Network > DNS**.
3. Select **Specify**.
4. Set the IPs for your primary and secondary DNS servers.
5. (Optional) If you have a local Microsoft domain on your network, enter its name for the **Local Domain Name**.
6. Select **Apply**.



Now you're all set to use the new servers.

Using Your Own Server

Setting up an internal DNS server can be lengthy and complicated, so it should only be attempted by someone with a solid understanding of how DNS works.

If you wish to manage your own DNS server, you can buy units specifically made for that purpose, such as a FortiDNS, you can devote one or more computers to the task, or you can set up your FortiGate unit to function as a DNS server. For more information about this FortiGate configuration, please refer to the FortiOS Handbook.

DNS for a Web Server

If your network includes any web servers or any other devices that require incoming traffic from the Internet and use URLs, you will have some more DNS concerns. The DNS master list for your site can be either on a third party server or on your own server.

For both types of servers, the security checklist from above can be used. If you are running your own server, be sure to have it located in a DMZ, to keep the incoming network traffic secure and segregated from your internal network. Also remember that domain registrars require at least two DNS servers, which should ideally be on two separate networks.

Resources

For more information about DNS, or to find some DNS tools, check out the following resources:

- The SANS Reading Room
- DNSstuff
- DomainTools
- DNS Toolbox

How do I create a Firewall Policy?

A firewall acts as a filter between your network and the outside world by scanning all network traffic and deciding what is allowed in or out. Firewalls are a well-known part of network security and in the last few years most operating systems include Firewalls as part of the system. Personal computer firewalls are usually fairly straightforward, you pretty much turn it on and let it do its thing.

Things get a bit complicated when more network devices are in play, especially if you want to restrict some traffic sources while allowing others. This is where firewall policies, also called security policies, come into play on your FortiGate.

The FortiGate Firewall

FortiGates, like most firewalls, operate on the basic idea that only traffic that is expressly permitted is allowed. That's why all FortiGates start out with a default deny policy that cannot be deleted, which is used as a catch-all for traffic that is not specifically set up as allowed. Most FortiGates also have a default policy that allows traffic from the LAN to the Internet.

These two policies do allow basic access for your network, but for a more complex network you'll need to know how to put together a specialized or more specific policy.

The Who, What, Where, and How of Firewall Policies

The first part of the policy's configuration is setting a few important fields. These fields act as filters to make sure the policy handles only the intended traffic.

- **Incoming interface:** FortiGate interfaces can be seen as one side of a bridge between two networks and each interface has its own MAC address and internal IP address. The incoming interface is either a single physical port or a switch, containing multiple ports, that listens for incoming traffic.

In our example, this would be the default LAN or internal interface (the name differs depending on which FortiGate model you have).

- **Source address**: This field sets which IP addresses traffic are allowed to send traffic through this policy. Addresses in this field must be predefined firewall objects. They can be specific IP addresses, ranges, subnets, Fully Qualified Domain Names or geographical locations (countries).

  In our example, this will be the range of addresses on the network's subnet. You could also select the option all, but using a firewall address is the best practice, as it ensures that only traffic from your subnet is allowed.
- **Outgoing interface:** This field determines the interface that the traffic for this policy is being sent out on.

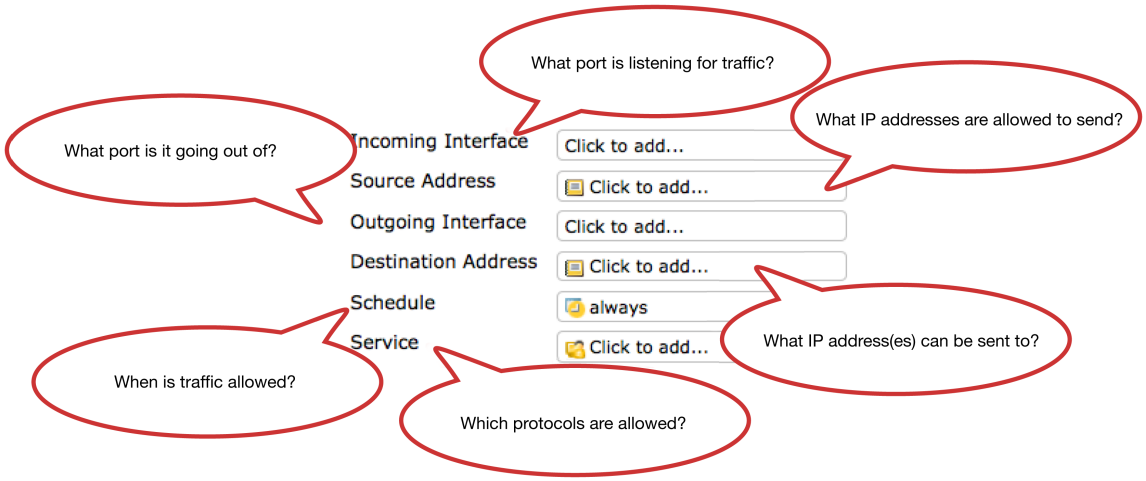
  In our example, this will be WAN1, which is typically the interface used to connect to the Internet.
- **Destination address**: This field controls the IP addresses that can be reached by traffic using this policy.

  In our example, this will be all, which will allow access to all websites on the Internet.
- **Schedule:** This field deals with when traffic is allowed to use this policy.

  For our example, we'll use a custom schedule that allows traffic on Monday, Tuesday, Wednesday, Thursday, and Friday, between 9AM and 5PM. Custom schedules can be created by going to **Firewall Objects >Schedule > Schedules**.
- **Service:** This field controls the protocols which can be used, such as HTTP, FTP, and SIP.

  In the example, we'll select HTTP, HTTPS, and DNS. It is important to remember to allow the DNS protocol since it is required for your computer to find websites.

To keep track of what you've learned so far, here's a quick "cheat sheet" graphic you can use.



Finally, make sure that the action is set to ACCEPT, which allows traffic to flow through the policy.

You can use the DENY option if there is traffic you want to prevent from getting through the firewall. For example, if you have identified the IP address of an attacker, you can drop any traffic from that IP.

If you are planning to create a number of firewall policies, you should know how the FortiGate matches traffic to a firewall policy. The FortiGate starts at the top of the policy list and works its way through each of the policies until it finds one that matches all six of the mentioned fields. When you are creating a policy,

you need to keep in mind the policies that will come before and after it. For example, make sure that you don't have one policy accepting traffic at the top that a different policy is meant to block.

You'll find more information about ordering policies below.

Address Translation

You will want to enable Network Address Translation (NAT) in a number of scenarios. These may include:

- You want to hide the addresses of your internal network from the Internet.
- You have fewer public IP addresses than devices that need to use them.
- You have two subnets that need to communicate that share an IP address range.

Logging Options

Choosing a logging option is also part of the firewall policy. In most cases, just logging security events is sufficient, in order to avoid dedicating too much memory to logging.

Security Profiles

Finally, security profiles and sensors are selected for the policy's traffic; however, we'll save talking about these features until we get to the layer of the network that they are involved with.

Ordering Policies

Once you've created your firewall policy, the final step before you can start using it is to make sure that the correct policy is used for all traffic that goes in or out of your FortiGate. When ordering policies, it is best to do the following:

- Custom DENY policies should be placed first so there is no chance that matching traffic will get through.
- VPN and other user identity-specific policies should be before policies that are not identity-specific.
- For all other policies, keep the more specific policies before general policies, so that traffic matching the specific policy is not accepted by the general one accidentally.

How to build a better policy

As networks become more advanced, so do the demands placed upon your firewall. As such, it is equally important to know how to make a firewall policy work, and to make it work well.

Improve Your Design

Just because a firewall policy works doesn't mean that it's design is perfect. Since firewalls play such a key role in keeping your network secure, it's important to ensure that there are no holes in the configuration. Keeping that in mind, here are a couple of best practices that could help you, both with new policies as well as any older policies you may have kicking around:

- When you create a new policy, start with the basics, ensuring that the policy works before adding the more complicated parts, like security features. While it may take more time to configure, starting with the basics makes it easier to pinpoint any problems that occur down the line, as it less likely you will encounter multiple issues at the same time.
- Avoid using the "ANY" setting as a service. Instead, only allow the services that your network users will require. Be sure to always allow DNS for any Internet access policy.
- Likewise, avoid using the default "all" setting for source addresses, unless you are creating a policy for incoming requests from the Internet. Instead, create a firewall address (a type of firewall object) that matches the addresses that are allowed to send traffic.
- When creating firewall addresses or other objects, give them a specific name that helps to identify the object in the future. For policies, use the Comment field to for the same purpose. This will make it easier to tell, at a glance, the purpose of each policy.
- When creating a policy that has user authentication, select a user group in the policy instead of a specific user account, so that if a new user is added to the group they will automatically be included in the policy without having to edit the policy directly.
- For the same reason, groups should also be used for firewall addresses, virtual IPs, and services if more than one is used in the policy.
- Only use logging as necessary - it is usually recommended to just log security events and use FortiCloud to store your logs. If you have to troubleshoot issues later, you can easily increase logging temporarily until the problem is found.

Policy Housekeeping

It's very common for policies to be added as a network evolves; it is less common for policies to be removed as they become unused or irrelevant.

If you are using numerous firewall policies, ensure that you don't have older policies kicking around that aren't in use. Not only could they cause unintended issues with valid traffic, they could also potentially become security vulnerabilities. It's easy to clear unnecessary policies if you've followed the best practices listed above, since you'll be able to see, at a glance, the purpose of each policy. However, even if you haven't, there are still a few things you can do to make it easier to decide if a policy should stay or go.

> Before you delete any policies or make any major changes, create a backup of your current FortiGate configuration. Store and label the configuration in such a way that you can find it again easily if needed.

1. Use the Section view in the policy list to show which policies have the same source and destination interface. If two interfaces have a large number of policies connecting them, there is a good chance that some are no longer necessary. If you have a FortiManager, you can use its Policy Check feature to look for duplicate policies, duplicate objects, or partially overlapping/shadowed policies, which are all candidates for deletion.
2. Examine any policies that aren't currently processing traffic to determine if they are still in use. You can do this a number of ways. In the policy list, you can use the Sessions column to show any active sessions that are currently being processed, and you can use the Count column to show you the total amount of traffic that hit this policy since the last reboot. You can also use the historical traffic logs to see when the policy was last used, or if it has ever been used at all.
3. Look at any policies located at the bottom of the list. A FortiGate starts at the top of the policy list and works its way through each of the policies until it finds the best match for the incoming traffic. Because of this, any policies at the bottom of a long policy list are less likely to be handling traffic than those at the top.

4. Test the policies you want to keep by generating some traffic and verifying in the logs that the intended policy processed that traffic. Just because traffic reaches its destination doesn't mean it gets there using the intended policy.

Other Firewall Tips

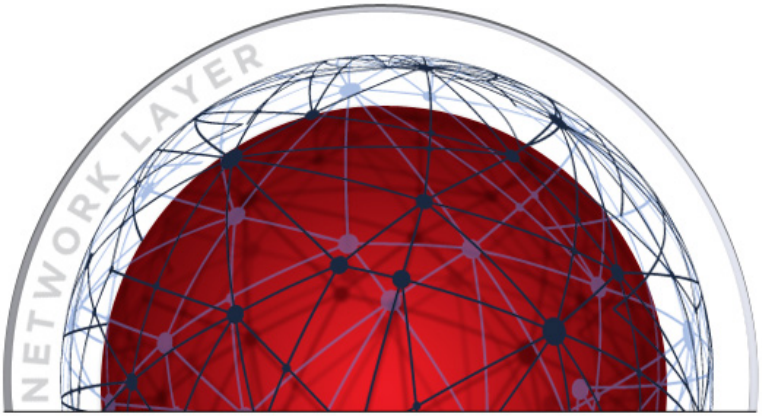
- When you upgrade your firmware from a previous version, read the Release Notes for the new version to find out if the policy process has changed. If there are changes (as with upgrades to the newly released FortiOS 5.2), be sure to review your policies to make sure they will still work as intended.
- Remember that users are unlikely to complain when they are getting more access than they should, but will definitely let you know when they are getting less access than they should.
- A simple solution is better than having a bunch of pieces cobbled together, even if the end result is the same. Take the extra time and effort to find these solutions, as they can simplify your configuration, saving you potential headaches in the future.

FortiGate Resources

For more information about FortiGate firewall policies, check out the following resources:

- Video: Basic Firewall Policies
- The FortiGate Cookbook: Creating security policies
- The FortiOS Handbook: Firewall for FortiOS 5.2
- Best Practices for FortiOS 5.2
- Whitepaper: Making Smart Policies

How Do I Protect Against External Attacks?



The network layer

Network layer security focuses on external threats that are able to bypass the firewall layer. Your FortiGate has two main features that deal with these threats: the Intrusion Prevention System (IPS) and Denial of Service (DoS) protection.

What are IPS and DoS protection?

IPS protects your network by actively seeking and blocking external threats before they can reach your network devices. These attacks are able to bypass the firewall because they use authorized protocols and addresses; for example, an attacker could use port 80, which is allowed for HTTP traffic, in an attempt to exploit a vulnerability on one of your network devices or applications. Adding an IPS profile to your security policies protects traffic flow by using signatures to recognize a variety of attacks as the traffic attempts to access the network.

While IPS targets attackers attempting to bypass your firewall, DoS protection deals with Denial of Service attacks, which aim to consume your firewall's resources so that they can't be used by anyone else. On a FortiGate unit, you create a DoS policy and associate it with a specific network interface so that external attacks are blocked from reaching that interface.

How to protect your network

To protect your network you must first enable IPS and DoS protection. With these security features active, you must then maintain a FortiGuard IPS subscription to ensure that they remain up-to-date. As long as you maintain the FortiGuard IPS subscription, you should be able to use one of the default IPS profiles and a basic DoS policy to keep your network safe.

Also consider the following tips to further protect your network:

- Only use the signatures that apply to your network. For example, you should include signatures that protect software installed on your network devices, but exclude those for other software. This saves the network resources that would otherwise be consumed scanning for attacks that can't affect you.
- If there is a network device or service that can be accessed from the Internet, block any signatures that correspond to that device or service. For example, if you have a web server, block all signatures related to web servers. Include all applicable signatures, even those of less severity, to avoid leaving any openings.
- To get the best protection from a DoS policy, determine the appropriate threshold level. A threshold level defines the maximum number of allowed sessions/packets per second.

  A DoS policy searches for anomalies in the packets, which can occur even in the absence of an attack. Because of this, setting the threshold automatically to 1 is not the best solution.

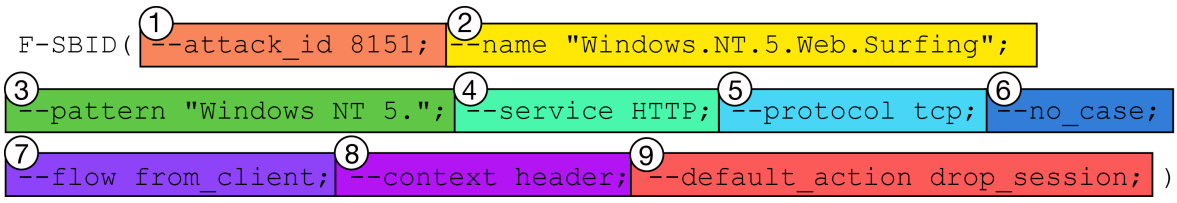
  To find the best threshold for your network, create a DoS policy, with the action set to Pass, and enable logging. By looking at the logs, you can figure out when normal traffic begins to generate attack reports. Then all you need to do is set the threshold above this value with the appropriate margin for your network.

The anatomy of a custom IPS signature

The FortiGuard signatures database is updated regularly, so you will have sufficient network security using only the aforementioned predefined signatures. However, you can also create custom signatures to protect against attacks that don't have a FortiGuard signature or to block unwanted behavior that is unique to your network.

All custom signatures have the same header: F-SBID( ). Keywords are entered between the brackets to instruct the FortiGate. Each keyword begins with two dashes (--) and ends with a semi-colon (;).

For example, the following signature blocks traffic from PCs running on older Windows operating systems using NT 5 (an operating system kernel that connects applications to the computer's hardware), including Windows XP and Windows Server 2003. Because these operating systems have reached end-of-life, devices using them are more likely to have been compromised to carry out attacks as part of a botnet.



#	Keyword	Value Description
1	attack_id	This number is used by the FortiGate for identification. You can either choose one yourself or let the FortiGate assign it for you. Values must be between 1000 and 9999.
2	name	All signatures require a unique name. In the example, the name clearly indicates the signature's purpose, i.e. blocking web traffic from any computer that uses any version of the Windows NT 5 kernel.

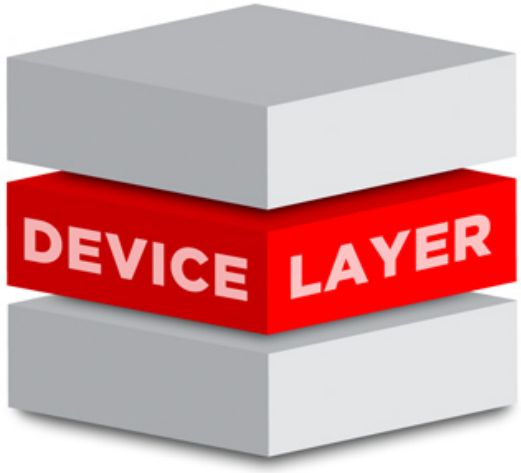
3	pattern	The pattern is what the FortiGate will look for in the traffic. In this case, it will look for packets that contain "Windows NT 5."
4	service	The signature includes a service value to indicate which service will be monitored; in the example, HTTP traffic.
5	protocol	The protocol value TCP is added to avoid unnecessarily scanning UDP and ICMP traffic.
6	no-case	By default, patterns are case sensitive. Adding this value ensures that case sensitivity is ignored, so that "windows nt 5" is also considered a match. Unlike other values, this part of the signature does not require a keyword.
7	flow	This value tells the FortiGate which direction of traffic to monitor.
8	context	This value tells the FortiGate to check the header of the packet for the pattern match.
9	default_action	This tells the FortiGate to drop any traffic that matches the pattern.

These are the core parts of a custom signature. More keywords are available for a variety of functions, which can be found in the Security Profiles Handbook (see the link below).

FortiGate Resources

- The FortiOS Handbook: Security Profiles for 5.2
- The FortiOS Handbook: Security Profiles for 5.0
- Inside FortiOS: Intrustion Protection System (5.2)
- Inside FortiOS: DoS Protection (5.2)

How Do I Keep Network Devices Secure?



While wired networks certainly have their own challenges (many of the precautions here are applicable to wired devices), it is wireless that really changed this layer's landscape. The biggest change that came with wireless is the rise of BYOD: bring your own device.

BYOD (not to be confused with BYOB) refers to employees using their own personal devices - such as laptops, tablets, and smartphones - to access the network at work. According to a Unisys study conducted by IDC in 2011, nearly 41% of the devices used to obtain corporate data were owned by the employee. It's hard to imagine that this number hasn't increased in the last four years.

Because of BYOD's increase in popularity, today's networks often include a myriad of different device types. Adding more devices and device types causes both the network's complexity and the number of potential threats to increase. This is why it is vital not only to protect each device but also take measures to protect the rest of the network from each device.

Protecting Each Device

The first steps of protecting the device layer occur on the device itself. Most computers these days have their own built-in firewall, which should be used regardless of FortiGate protection. Anti-malware software should also be run on the device regularly, with scans scheduled for a time when it isn't in use. Finally, you should regularly apply updates for both operating systems and apps, to ensure that any known vulnerabilities are dealt with.

One easy way to protect the devices on your network is to use FortiClient. FortiClient extends the power of FortiGate's unified threat management to endpoints on your network. This includes features such as AntiVirus, web filtering, two-factor authentication, and being able to securely connect to either SSL or IPsec VPNs.

FortiClient is available for Windows, Mac OS X, iOS, and Android, and can be set up quickly. After being installed, it automatically updates its virus definition files, does a full system scan once per week, and much more. A FortiGate can make sure that all devices using FortiClient have the current updates.

FortiClient can be downloaded at www.forticlient.com.

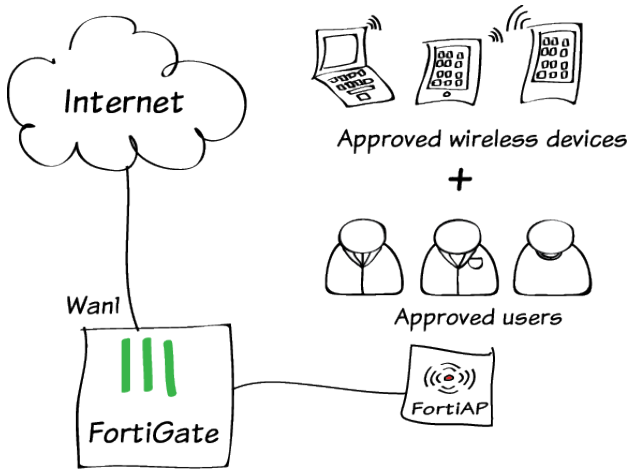
Knowing Thy Network

The next step to managing devices is figuring out what devices are actually out there in need of being managed. FortiGate interfaces, including wireless SSIDs, can identify the devices on the networks that they connect to. This gives you a list of all the devices on your network. Your FortiGate is also able to identify each and which operating system they use, to a fair degree of accuracy.

Device Management

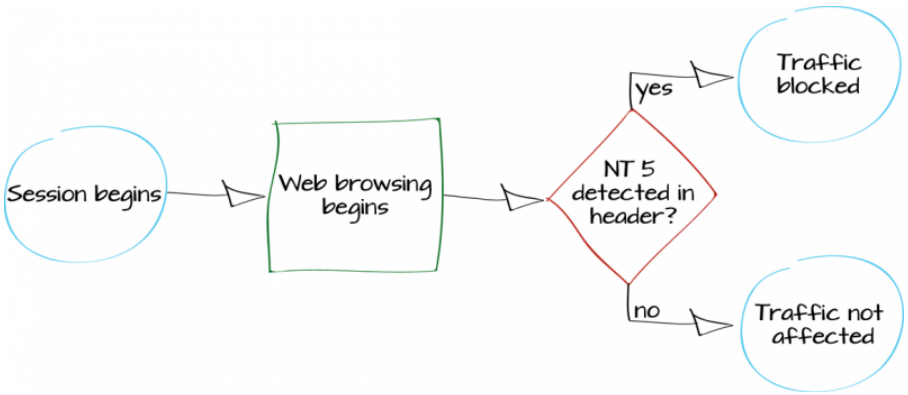
Once you know what devices are out there, you can figure out if there's anything that shouldn't be allowed in the first place. Below are three recipes from the Fortinet Cookbook that showcase what a FortiGate can do to help with this.

Recipe 1: Allow or block different types of devices, to make sure only the right ones can connect, even if they are being used by the same person.



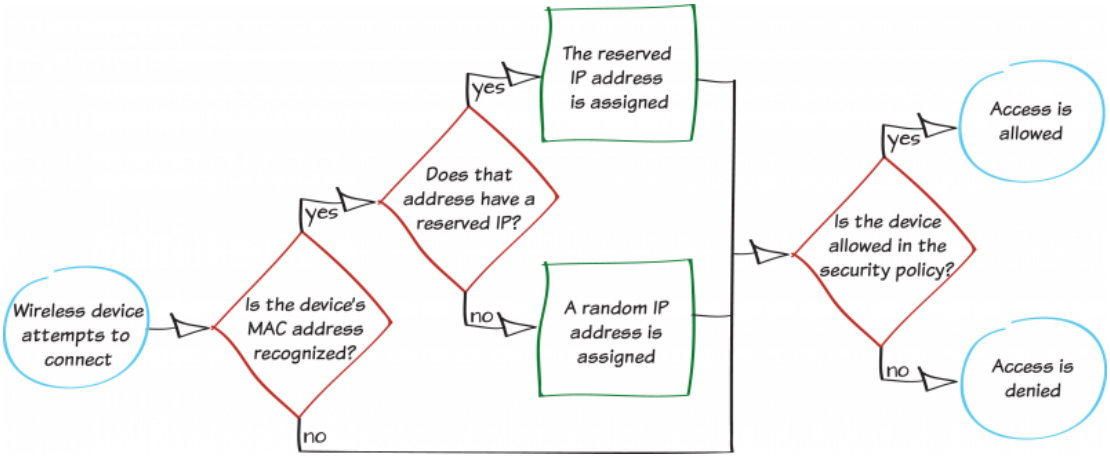
BYOD for a user with multiple wireless devices

Recipe 2: Block web traffic from computers running on an outdated OS using application control, such as Windows XP.



Blocking Windows XP traffic

Recipe 3: Create custom device definitions or groups, allowing you to determine what network access devices have on a case-by-case basis.



MAC access control

Let People Know

In 2013, a Fortinet Internet Security Census found that 51% of the partipants said they would would contravene company policies restricting use of own devices, cloud storage and wearable technologies for work. To help avoid this problem, make sure that you let users know what your policies are and why you have them.

We'll talk more about network users in the next installment.

Fortinet Resources

- Managing Devices (FortiOS Handbook for 5.2)
- Managing Devices (FortiOS Handbook for 5.0)
- FortiClient Administration Guides